group based on at least one criterion selected from the group consisting of language, age, affiliation, and password creation policies;

incorporating said relevant patterns into said probabilistic context-free grammar;

utilizing probability smoothing to assign additional probability values to other keyboard patterns for other password strings not found in said plurality of password strings, wherein said step of utilizing probability smoothing is achieved by an equation

$$Prob(p) = Prob(s)\frac{N_i + \alpha}{\sum N_i + C\alpha}$$

where Prob(s) is the probability of a keyboard shape s given the length of the keyboard pattern, Ni is the number of times an ith keyboard pattern of a shape s was found, $\alpha$ is a smoothing value, $\Sigma N_i$ is a sum of counts of the keyboard patterns found for the shape s, and C is a total number of unique patterns for the shape s;

receiving one or more input dictionaries containing a plurality of sequences of alpha characters;

optimizing a primary dictionary of said one or more input dictionaries based on size and content of said primary dictionary;

assigning an additional probability value to said primary dictionary, wherein an effectiveness of said primary dictionary is measured by coverage and precision of said primary dictionary cracking said targeted password,

said one or more input dictionaries further including a secondary dictionary for cracking said targeted password;

generating password guess strings in decreasing estimated probability via said probabilistic context-free grammar by utilizing said plurality of sequences of alpha characters;

accessing a login interface to the secured user account; and

applying said password guess strings from said computer processor sequentially to said login interface, whereby authentication of the user can be achieved.

* * * * *